MINISTERO DELLA PUBBLICA ISTRUZIONE
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
Istituto d'Istruzione Superiore "U. Midossi"
Via F. Petrarca s.n.c. – 01033 Civita Castellana (VT)
Tel.: 0761-513671 **fax:** 0761 591145 **pec:** VTIS007001@istruzione.it

Al personale Amministrativo

Oggetto: Linee Guida in materia di Sicurezza del Trattamento dei dati per il personale amministrativo impartite dall'Istituto d'Istruzione Superiore "U. Midossi", nella persona del dirigente scolastico *pro tempore* prof. Alfonso Francocci, quale Titolare del trattamento.

Gentili colleghi,

dal 25 maggio 2018 è entrata in vigore la normativa Europea in materia di protezione dei dati, Regolamento Europeo 20167679 c.d. "GDPR".

Le novità contenute nel dispositivo legislativo, valido in tutti i Paesi Membri, l'Informativa relativa al Trattamento dei Dati e tutta la documentazione utile è riportata nella sezione del sito web della scuola, sezione Privacy.

Tutto il personale è tenuto a conoscere e a rispettare i termini attuativi della norma, prendendo visione del materiale pubblicato e attenendosi alle istruzioni in esso contenute.

In particolare, si raccomanda:

- la compilazione delle liberatorie/prestazione del consenso per l'uso di media nei quali siano ripresi gli alunni (a inizio anno scolastico e/o quando si presentano occasioni particolari);
- l'informativa sul trattamento dei dati e il consenso esplicito in tutte le procedure amministrative con terzi (ad esempio affidamento servizi ad agenzie viaggi, consulenti, tirocinanti, formatori etc), nella compilazione di atti estranei alle finalità perseguite dall'istituto recanti dati particolari (ad esempio PDP, PEI degli studenti) e in tutti i casi nei quali si reputasse necessario secondo norma.

Al fine di assicurare a tutti gli Interessati un trattamento dei dati lecito e garantito da adeguate misure di sicurezza, il Dirigente Scolastico prof. Alfonso Francocci

Comunica

le presenti linee guida contenenti la descrizione delle misure operative cui tutto il personale Amministrativo dovrà scrupolosamente attenersi al fine di garantire la sicurezza dei dati personali dei soggetti interessati.

Definizioni

Costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la

modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

Ai sensi dell'art. 4.1 GDPR, si intende per dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Rientrano nella categoria dei dati particolari di cui all'art. 9 del GDPR quei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

È definito Titolare del trattamento la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (cfr. art. 4.7 GDPR).

Per responsabile del trattamento si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (cfr. art. 4.8 GDPR).

Misure operative generiche

Nello svolgimento delle sue mansioni, il personale amministrativo autorizzato dovrà:

- accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- trattare i dati personali in modo lecito e secondo correttezza;
- raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli solo per operazioni di trattamento compatibili con le finalità connesse all'attività svolta;
- verificare che i dati siano esatti e, se necessario, aggiornarli;
- verificare che i dati siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservare i dati in forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati, e comunque nel rispetto delle *"Linee guida per gli archivi delle istituzioni scolastiche"* predisposte dal Ministero per i Beni Culturali e le Attività Culturali, messe a disposizione dall'Istituto Scolastico;
- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- informare prontamente il Titolare o il Responsabile per la Protezioni dei Dati dell'Istituto (RPD), di seguito indicato, di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;

- non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare e, comunque, senza avere la certezza della loro identità;
- non lasciare a disposizione di estranei documenti o supporti di memorizzazione (cd, dvd, pen drive) che contengono dati personali comuni o particolari;
- accertarsi della distruzione di documenti inutilizzati contenenti dati personali comuni o particolari;
- non abbandonare la postazione di lavoro, senza aver provveduto a custodire in luogo sicuro i documenti contenenti dati personali;
- collaborare con il Responsabile per la Protezione dei Dati dell'Istituto per aspetti specifici relativi ad ogni nuova attività che comporti il trattamento dei dati personali. Misure operative specifiche all'utilizzo di tecnologie informatiche;
- scegliere per i diversi software gestionali (area Personale, area Didattica, eccetera) una password che sia composta da otto caratteri e non facilmente intuibile, evitando che contenga riferimenti alla propria persona (es. proprio nome o di congiunti, date di nascita, ecc.);
- curare la conservazione della propria password dei software gestionali e non comunicarla per alcun motivo a soggetti terzi;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password dei software gestionali;
- adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al Trattamento di Dati Personali (mail, account per piattaforme terze, eccetera);
- effettuare il log-out dai software gestionali e, laddove presenti, da sistemi di autenticazione di rete al termine di ogni sessione di lavoro;
- spegnere correttamente il computer al termine di ogni sessione di lavoro al fine di agevolare, se utilizzati, l'azione di software specifici di congelamento delle configurazioni degli stessi;
- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- nella comunicazione multimediale con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto;
- nell'utilizzo della posta elettronica non aprire documenti di cui non sia certa la provenienza e controllare accuratamente l'indirizzo dei destinatari prima di inviare e-mail contenenti in allegato o nel corpo del messaggio dati personali;
- nell'esercizio delle proprie mansioni utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, presenti negli uffici di segreteria: ufficio segreteria del personale, ufficio di segreteria didattica, ufficio affari generali, eccetera), in quanto tali attrezzature sono regolarmente sottoposte a rigide misure di sicurezza e in linea con le misure minime di sicurezza ICT emanate dall'AGID. Qualunque violazione delle modalità sopra indicate dà luogo a precise responsabilità, ai sensi delle normative vigenti.

Misure operative specifiche

Il personale amministrativo dovrà, altresì, operare del rispetto delle seguenti prescrizioni:

- controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza;
- conservare sempre i dati relativi al trattamento di cui si è incaricati in apposito armadio/archivio assegnato, che dovrà sempre essere chiuso a chiave dopo l'utilizzo;
- prima di procedere alla raccolta e al trattamento dei dati, fornire sempre l'informativa all'interessato e conservare il modello opportunamente firmato dall'interessato o da chi lo rappresenti;
- sarà possibile accedere ai soli dati personali, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico;
- i documenti o gli atti che contengono dati particolari e/o giudiziari devono essere conservati in appositi archivi (ad esempio stanze, armadi, schedari, contenitori in genere) che dovranno rimanere sempre chiusi a chiave. Le copie delle chiavi saranno nella disponibilità del Dirigente Scolastico e del DSGA;
- qualora dovessero giungere richieste telefoniche di dati particolari da parte dell'Autorità Giudiziaria e/o organi di Polizia, si deve richiedere l'identità del chiamante. Si dovrà, quindi, avvertire il Dirigente Scolastico o il DSGA che provvederanno a ricontattare il chiamante in modo da avere la certezza sull'identità del richiedente;
- nella comunicazione di dati particolari adottare sempre procedure che permettano di garantire la sicurezza e la riservatezza delle informazioni anche mediante tecniche di anonimizzazione e di pseudonimizzazione;
- i documenti cartacei non più utilizzati, specie se particolari, devono essere distrutti o comunque resi illeggibili, prima di essere eliminati o cestinati;
- conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
- consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
- non consentire l'accesso ad estranei nelle aree in cui sono custoditi documenti cartacei o contengano supporti informatici di memorizzazione
- effettuare esclusivamente copie fotostatiche o su supporto informatico di documenti per i quali si è autorizzati;
- non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali comuni o particolari ma accertarsi che vengano sempre distrutte;
- non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;
- non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;

Trattamenti eseguiti con supporto informatico

Relativamente ai trattamenti effettuati con supporto informatico devono essere seguite le seguenti ulteriori prescrizioni:

- per l'accesso alla postazione di lavoro utilizzare le credenziali di accesso fornite e/o successivamente modificate;

- adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia di ogni altro dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, etc.): È FATTO DIVIETO DI COMUNICARE AD ALTRI LE PROPRIE CREDENZIALI DI ACCESSO;
- tutte le volte che si abbandoni la propria postazione di lavoro i pc e/o i terminali devono essere posti in condizione di non essere utilizzati da estranei. In particolare, si raccomanda di chiudere tutte le applicazioni in uso e di porre un blocco del sistema mediante password;
- spegnere sempre il PC alla fine della giornata lavorativa o in caso di assenze prolungate dalla postazione di lavoro;
- ove si dovessero riscontrare difformità dei dati trattati o nel funzionamento degli elaboratori occorre darne immediata comunicazione al Dirigente Scolastico;
- utilizzare sempre l'antivirus per verificare il contenuto di qualunque supporto di memorizzazione;
- aggiornare sempre l'Antivirus quando richiesto dal Software.

Regole per la scelta delle credenziali di accesso/Password

Nella scelta della propria password di accesso ai servizi informatici il personale dovrà:

- individuare una password che sia composta da otto caratteri e non facilmente intuibile, evitando che contenga riferimenti alla propria persona (es. proprio nome o di congiunti, date di nascita, ecc.).
- curare la conservazione della propria password del Registro
- informatico e non comunicarla per alcun motivo a soggetti terzi;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password del Registro Informatico;
- adottare le stesse cautele di cui sopra per le password di qualsiasi altra piattaforma software ad uso personale e potenzialmente interessata al Trattamento di Dati Personali (come ad esempio la mail, o l'account per piattaforme eLearning).

Si precisa che il titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal d. lgs. n.196/2003 e del Regolamento UE 2016/679. Tuttavia, le responsabilità per l'inosservanza delle istruzioni impartite dal Titolare del trattamento possono riguardare anche il personale di servizio che non rispetti o adotti le misure necessarie.

Dati di contatto del titolare e del responsabile per la protezione dati

Titolare del trattamento è l'Istituto d'Istruzione Superiore "U. Midossi", nella persona del dirigente scolastico prof. Alfonso Francocci, con sede in 01033 Civita Castellana (VT), Via F. Petrarca s.n.c.

Tel.: 0761-513671 Fax: 0761 591145 Pec: VTIS007001@istruzione.it

Responsabile della Protezione dei dati (R.P.D. – D.P.O.) è l'avv. Alberto Colabianchi.

Pec: albertocolabianchi@ordineavvocatiroma.org Email: s.colabianchi@studiocolabianchi.com

Civita Castellana, 11.11.2019 Il Dirigente Scolastico prof. Alfonso Francocci